Vysoká škola báňská – Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra telekomunikační techniky

Monitorování bezdrátových sítí

Monitoring wireless networks

2010 Ondřej Pavelka

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 5. 5. 2010 ……

Ondřej Pavelka

Poděkování

Za rady a připomínky při vypracování této bakalářské práce bych rád poděkoval panu Ing. Pavlu Nevludovi.

Abstrakt

Tato práce se snaží vysvětlit pojem „monitorování bezdrátových síti“ se zvláštním zaměřením na bezdrátové počítačové sítě. Práce zahrnuje podrobný popis protokolu SNMP, který je jedním z nejvýznamnějších protokolů určených pro monitorování počítačových sítí. Zahrnuje také informace o množství monitorovacích softwarových řešení a jejich srovnání, dále pak výběr monitorovacího software a jeho následnou implementaci na komerční bezdrátové síti opENet.

V závěru práce bych chtěl předvést výstupy z monitorovacích software, které jsem implementoval a také představit jaké výhody z toho plynou výhody, pokud je konkrétní síť monitorována.

Klíčová slova

Wi-Fi, monitoring, nagios, cacti, snmp, bezdrátové sítě

Seznam použitých symbolů a zkratek

Wi-Fi – (Wireless Fidelity) Zaručení kompatibility
SNMP – Simple network Management Protocol, protokol pro management síťových zařízení
Open source – Nekomerční licenční ujednání
UBNT – Ubiquiti networks, firma vyrábějící komplexní bezdrátové zařízení
OS – Operační systém
SMTP - Protokol pro odesílání pošty
RouterOS – Operační systém pro zařízení Mikrotik

Abstract

This work seeks to explain the term “monitoring wireless networks“ with a focus on wireless computer networks. It contains a complete description of SNMP protocol, which is one of the most significant protocols used to monitor computer networks. This work also includes different solutions for monitoring software and their price comparison; moreover, I will choose suitable monitoring software to implement on the commercial wireless network opENet.

At the end of the work, I would like to introduce the results of concrete monitoring software which I have implemented and I would like to present the advantages and disadvantages of monitoring this concrete network.

Keywords

Wi-Fi, monitoring, nagios, cacti, snmp, wireless networks

List of used symbols and abbreviation

Wi-Fi – (Wireless Fidelity) zaručení kompatibility
SNMP – Simple network Management Protocol
Open source – Nekomerční licenční udejnání
UBNT – Ubiquiti networks, company producing complex wireless devices
OS – Operation system
SMTP - Simple Mail Transport Protocol
RouterOS – Linux based operation system

Obsah

1 Úvod

V dnešní době hraje stále významnější roli internet. S jeho rozvojem roste stále více obliba bezdrátových sítí. Uživatelé chtějí být připojeni všude a za každých okolností. K masovému rozšíření internetu přispěl i rozvoj levných bezdrátových sítí. Během posledních několika let vznikly stovky nezávislých poskytovatelů internetu, a ti začali budovat své vlastní bezdrátové sítě. Tímto způsobem vzniklo i nemalé množství amatérských bezdrátových sítí.

Nasazení vhodného monitoringu je proces, který se liší na každé síti, a je nutné ho vytvořit individuálně. Monitoring slouží k nepřetržitému sledovaní stavu služeb a dostupnosti síťových prvků. U rozsáhlých sítí je třeba sledovat celou řadu údajů, tak abychom mohli efektivně řídit a managovat celou síť. Požadované informace nám například poskytuje protokol SNMP, který je u počítačových sítí standardem.

Tato bakalářská práce se zabývá výběrem a implementací vhodného monitorovacího software pro internetového poskytovatele. Tuto implementaci se pokusím prakticky otestovat na firmě opENet. Úkolem této práce je zajištění kvalitního monitoringu za účelem zlepšení dostupnosti internetu a zlepšení kvality poskytovaných služeb.

2 Cíl práce

Cílem této práce je porovnání monitorovacích produktů pro bezdrátové sítě. Po výběru jednoho nebo více produktů pak implementace a konfigurace na bezdrátové síti opENet za účelem monitoringu a zlepšení kvality bezdrátového internetového připojení.

3 Analýza současného stavu

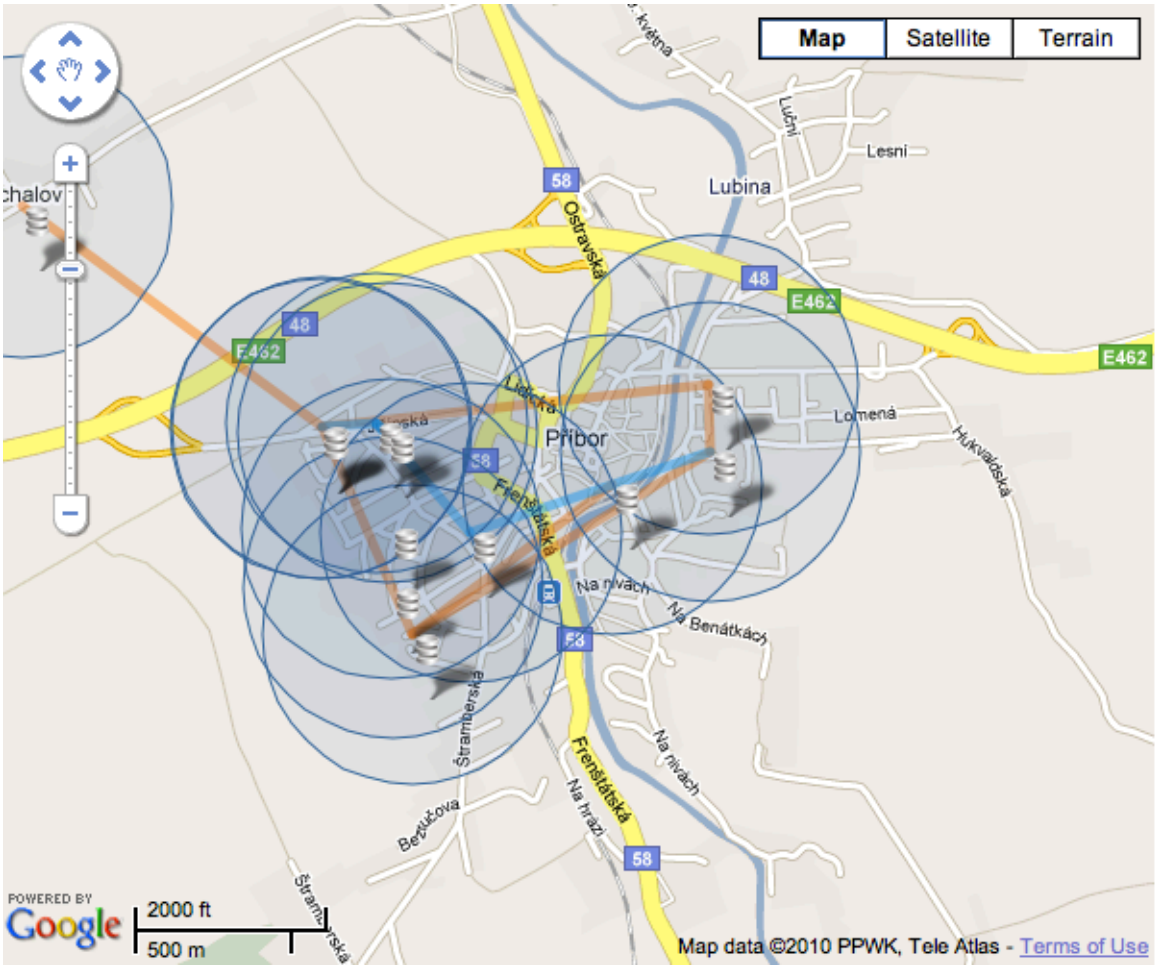
3.1 Seznámení s firmou opENet

Firma byla založena v červnu roku 2007. Na počátku bylo bezdrátově připojeno pouze několik známých majitele na tehdy drahou garantovanou ADSL linku jiného živnostníka. Postupně byla klientela rozšiřována, nakonec byla založena firma opENet s vlastní živností a povolením od Českého telekomunikačního úřadu. K dnešnímu dni čítá počet klientů kolem 120 domácností po celém městě Příbor a okolí. Majitel hodlá připojení stále udržovat, a zajišťovat jeho stále lepší kvalitu.

Obrázek 3.1 - Mapa Příbora a sídlo firmy

3.2 Struktura sítě

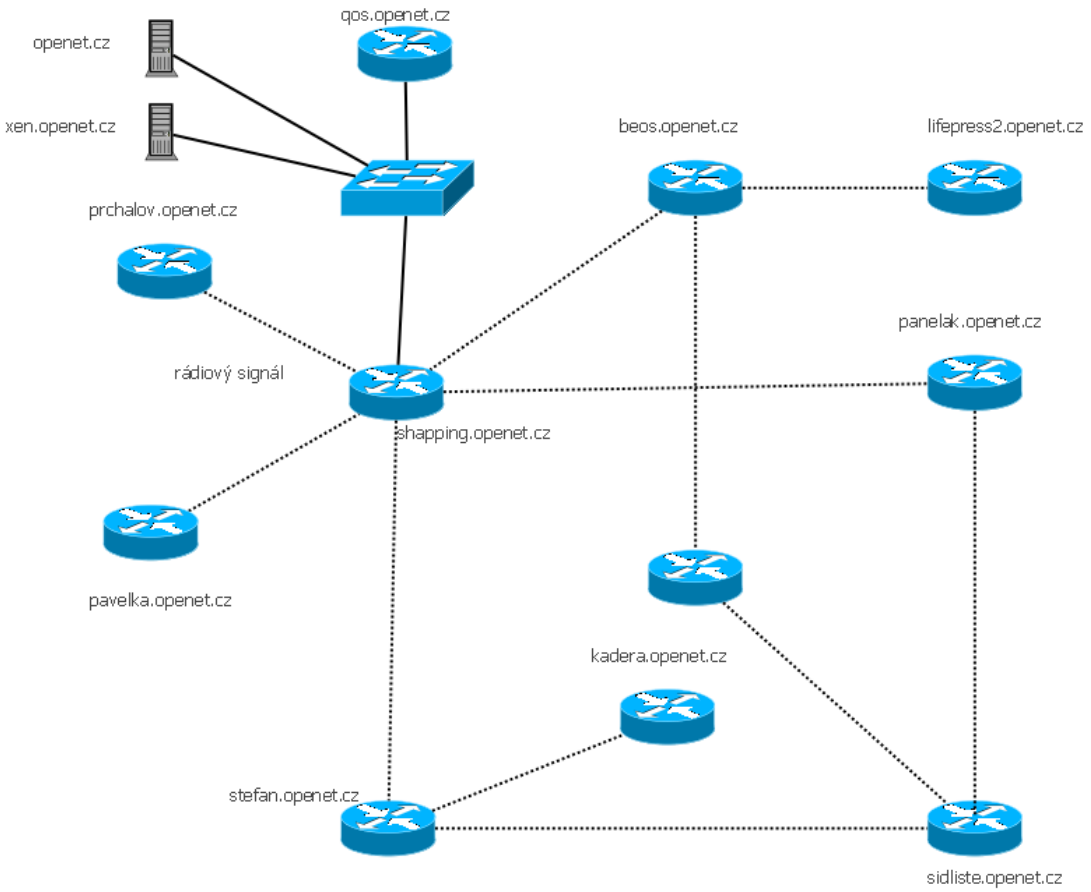
Jako hlavní konektivita slouží 10Ghz spoj Miracle od firmy MIRAMO s.r.o. Tento spoj je velice kvalitní, a po jeho dobu provozu, tedy zhruba 2 roky, nebyl zaznamenán jediný výpadek. Do budoucnosti je naplánována výstavba optické sítě na hlavní bod. Tato výstavba je plánována na červenec 2010. Aktuální konektivita má rychlost 20/20M bez agregace. Všechny páteřní spoje, tedy spoje mezi routery, jsou postaveny na volném pásmu s 5Ghz frekvencí a vertikální polarizací. Zhruba polovina klientů je připojena pomocí WA2200A access pointů na 2.4Ghz frekvenci, ale od této frekvence už bylo upuštěno vzhledem k velkému rušení na kanálech. Zbytek klientů je připojen buď v panelových domech přímo ethernetovým kabelem na páteřních bodech, nebo na 5Ghz. Většina zařízení na 5Ghz, která jsou používána, jsou od firmy UBNT, nebo přímo Routerboardy od firmy Mikrotik. Jako dva koncové routery jsou použity dva počítače s RouterOS softwarem. První router qos.openet.cz slouží jako hlavní router veřejných ip adres, a také jako hlavní firewall. Zde je také provedena priorizace jednotlivého datového provozu. Další router shapping.openet.cz slouží jako hlavní bezdrátový router. Zde jsou 4 bezdrátová rozhraní, a také je zde omezena rychlost jednotlivým uživatelům.



Obrázek 3.2 - Interaktivní mapa přístupových bodů umístěna na firemním webu

Další zařízení jsou dva servery. První server je UBUNTU 8.04, na kterém běží množství webových virtuálních serverů, ftp server, ssh server a celá řada linuxových aplikací. Druhý server je XEN server, tedy virtuální server. Na tomto serveru momentálně běží WM2003 server, kde je nainstalován doménový řadič, sdílení a mnoho dalších aplikací. Dále je v XEN serveru množství linuxových virtuálních serverů, které jsou používány na různé testovaní než na reálný provoz.

Protože je celá síť zakruhovaná, pro zajištění lepší dostupnosti je používán dynamický routovací protokol OSPF.



Obrázek 3.3 - Rozložení a propojení sítě

3.3 Použité zařízení

Celá síť byla budována po dobu tří let, a je stále ve vývoji. Po tuto dobu byly používány různé druhy zařízení. Po delším testování byla pro provoz vybrána zařízení od firmy Mikrotik, vzhledem k jejich relativně nízké ceně a široké možnosti nastavení. V síti jsou zařízení Mikrotik, např. RB133, RB333, RB433AH, RB433, RB600.

3.4 Požadavky monitorovacího software

Na základě výše uvedené analýzy současného stavu bezdrátové sítě opENet, od monitorovacího software vyžadujeme následující vlastnosti:

- Schopnost monitorovat síťová zařízení od různých výrobců
- Schopnost monitorovat celkově až 150 koncových klientů
- Schopnost jednoduše přidávat další zařízení
- Schopnost monitorovat různé výkonnostní ukazatele na různých zařízeních (cpu, paměť)
- Schopnost zasílání různých zpráv správci sítě
- Nízké pořizovací náklady
- Vizuální výstupy zatížení jednotlivých zařízení
- Upozornění na výpadky, změny signálu zařízení, přetížení linky
- Vzdálený přístup pomocí webového rozhraní
- Komplexní grafy jednotlivých uživatelů
- Monitorování serveru a jeho služeb

4 Výběr a porovnání vlastností SW pro monitorování

4.1 Přehled protokolů pro management a monitoring sítě

4.1.1 Protokol SNMP

Pro monitorování sítí existuje celá řada různých nástrojů nejrůznějšího typu. Hlavním protokolem pro management je protokol SNMP. Zkratka SNMP v angličtině zní „simple network management protokol“, tedy v překladu „jednoduchý protokol pro management sítě“. Termín SNMP označuje síťový protokol a standard architektury pro management a monitorování sítí TCP/IP nebo IPX.

Historie tohoto protokolu se datuje od roku 1990, a je schválen jako standard RFC1157. Hned po vypuštění první verze protokolu SNMPv1 se začíná pracovat na verzi SNMPv2. Ta má oproti původní verzi např. 64bitové čítače. Dnešní aktuální verze je protokol SNMPv3, a je schválen jako standard RFC2570, ve kterém je mimo jiné implementováno také šifrování přenosu a uživatelská autentizace.

SNMP protokol pracuje na vyšších aplikačních vrstvách OSI modelu. Je tedy závislý na nižších vrstvách OSI modelu, a musí být u daného zařízení podporován výrobcem.

4.1.2 Model Manager –Agent

SNMP je založen na komunikaci modelu manager a agent. Jedná se tedy o klasickou komunikaci klient-server. K získávání informací od agenta slouží tzv. MIB (Management Information Base). MIB je datová stromová struktura, která odpovídá danému zařízení. Tato struktura obsahuje definice a vlastnosti spravovaných objektů uvnitř sledovaných síťových zařízení.

4.1.2.1 SNMP Manager

Je program, který běží na síťové stanici umístěné v síti. Funkce SNMP manageru spočívá v dotazování jednotlivých SNMP agentů pomocí SNMP operací. Cílem je získat informace ze SNMP agentu, které pak SNMP manager dále zpracovává v podobně grafů, uložení do databáze, tvoření statistik, spuštění různých alarmů a podobně.

4.1.2.2 SNMP Agent

Je to malý program, běžící na síťovém zařízení, které chceme monitorovat. SNMP agent pomocí vlastních implementovaných funkcí zachycuje a monitoruje různá data o svém stavu, a dále je poskytuje SNMP manageru. Aby SNMP manager získal informace ze SNMP agenta, musí projít celou stromovou strukturu MIB a získat informace, které k danému objektu potřebuje.

Informace, které agent zaznamenává, mohou být také vyslány bez vyžádání managerem, pokud SNMP agent detekuje určitou chybu nebo nějaký alarm. Tato informace se jmenuje trap.

4.1.3 SNMP operace

GetRequest[6] **–** žádost o data, kterou posílá SNMP manager SNMP agentovi. Tato data manager zasílá, aby zjistil stav nějakého objektu agenta. Při jedné žádosti může manager požádat o informace více objektů, tím se také snižuje náročnost na komunikaci v rámci sítě. Jedná se čistě o operaci READ.

GetNextRequest – obdoba operace GetRequest, tzv. žádost o další data. Protože informace jsou hierarchicky uloženy v datové struktuře, jde o žádost o nižší úroveň v MIB struktuře.

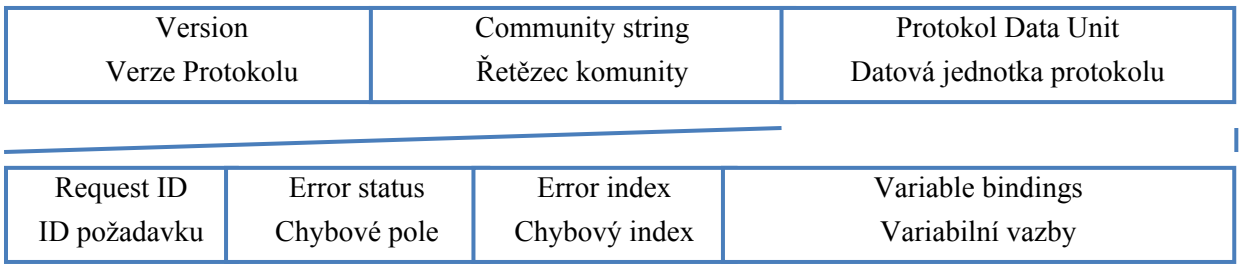
GetRespons – tímto příkazem odpovídá SNMP agent SNMP manageru společně s daty, které si SNMP manager vyžádal.

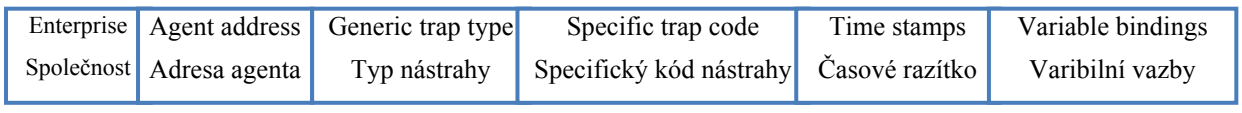
SetRequest – tento příkaz nastavuje nějakou hodnostu v MIB agentu. Tímto příkazem můžeme zařízení managovat, tzn. můžeme nastavovat různé hodnoty konfigurace. Ne všechna zařízení tento mod podporují. Jedna se o typický příklad operace WRITE.

TRAP – tento příkaz je vyslán SNMP agentem a upozorňuje SNMP managera na výskyt nějaké události, alarmu nebo problému. Tento příkaz si sami výrobci modifikují a upravují tak, aby co nejvíce vyhovoval zařízení, pro který je určeno. Např. u bezdrátových zařízení to bude síla signálu, kolize ip adres, vysoká odezva apod.

4.1.4 Formát SNMP zprávy

SNMP zpráva se skládá z hlavičky zprávy a vlastní PDU (Protocol Data Unit). V hlavičce zprávy je vlastní verze zprávy (Version) a název komunity (Community string). Datová část zprávy SNMP obsahuje jeden ze specifikovaných SNMP příkazů operací – GetRequest, GetNextRequest, GetRespons, SetRequest, Trap.





Obrázek 4.1 - Formát SNMP zprávy

Jednotlivá pole mají následující význam:

- ***Request ID*** *- přiřazuje požadavky s odpověďmi.*
- ***Error status*** *- indikuje chybu a její typ.*
- ***Error index*** *- přiřazuje chybu dané proměnné z pole variable bindings.*
- ***Variable bindings*** *- obsahuje vlastní data SNMP PDU, přiřazuje daným proměnným jejich aktuální hodnoty (vyjma Get a GetNext příkazů).*

SNMP PDU typu trap se trochu liší a obsahuje tato pole:

- ***Enterprise*** *- identifikuje typ objektu, který vygeneroval trap.*
- ***Agent address*** *- je adresa objektu, který vygeneroval trap.*
- ***Generic trap type, Specific trap code*** *- identifikují typ a kód trapu.*
- ***Time stamp*** *- čas mezi poslední reinicializací sítě a vygenerováním trapu.*
- ***Variable bindings*** *- seznam proměnných, které obsahují relevantní informace k danému trapu.*

4.1.4.1 Bezpečnost přístupu

Důležitou součástí SNMP komunikace je systém zabezpečení přístupu k objektům. Jedná se vlastně o definování přístupových práv k jednomu SNMP Agentu z různých SNMP Managerů. Systém je v principu velice primitivní, každý příkaz obsahuje v sobě i tzv. Community String, který funguje jako kombinace uživatelského jména a hesla.

V praxi je to zařízeno tak, že správce zařízení definuje jeden Community String pro read-write přístup k objektům uvnitř zařízení a jeden Community String pro pouze omezený read-only přístup. Jestliže Community String, obsažený v SNMP příkazu, souhlasí s jedním nebo druhým, definovaným pro zařízení, přístup k zařízení je umožněn s odpovídající úrovní přístupu. Nesouhlasí-li, požadavek je odmítnut.

Nejpoužívanější "default" Community String u SNMP zařízení je "public" pro read-only přístup a "private" pro read-write přístup. Je však jen třeba dávat pozor na rozlišení velkých a malých písmen, což je trochu nezvyklé.

4.1.5 Praktické použití SNMP

Každý SNMP objekt zařízení musí mít unikátní jméno, které je použito pro SNMP operace. Každé zařízení, které podporuje SNMP protokol, má vlastní MIB datovou stromovou strukturu. Přesná hierarchie této struktury je většinou volně ke stažení na webových stránkách výrobce. Na obrázku č. 4.2 můžeme vidět OID čísla objektů Queue Tree zařízení Mikrotik.

OID specifikuje následující formát:

.1.3.6.4.1.14988.1.1.2.2.1.**X**.**Y**

kde **X** specifikuje[8]:

2	pojmenování queue (pokud není zadáno, je shodné s target IP adresou)
3	target IP adresa
4	target IP maska
5	destination IP adresa
6	destination IP maska
8	**přijaté bajty**
9	**odeslané bajty**
10	přijaté pakety
11	odeslané pakety

a **Y** specifikuje hodnotu, kterou hledáme.

```
[ondra@shapping.openet.cz] /queue> simple print oid
Flags: X - disabled, I - invalid, D - dynamic
 0    name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.127
      bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.127
      bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.127
      packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.127
      packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.127

 1    name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.128
      bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.128
      bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.128
      packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.128
      packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.128

 2    name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.80
      bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.80
      bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.80
      packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.80
      packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.80
```

Obrázek 4.2 – Příklad OID struktury pro výpis z RouterOS

4.2 Seznam komerčních software pro monitoring

4.2.1 CiscoWorks CiscoView

Společnost Cisco je zaměřena na služby v oblasti sítí, a to jak na hardware, tak software. Pro tuto správu nabízí specifické nástroje. Jedním z nich je CiscoWorks CiscoView, který je komplexní aplikací pro centrální správu a monitoring Cisco zařízení.

4.2.2 WhatsUp Gold

WhatsUp Gold nabízí silné a efektivní nástroje pro správu sítí, monitorování služeb a různých komunikačních protokolů. Jeho základem je protokol SNMP nebo funguje prostřednictvím WMI protokolu. Dokáže monitorovat například zaplnění disku, vytížení paměti, zatížení procesu apod. Na události také reaguje prostřednictvím e-mailu, sms a dalších služeb.

4.2.3 HP OpenView Network Node Manager

Network Node Manager (NNM) od společnosti Hewlett-Packard představuje ucelené řešení pro správu a management sítě. Poskytuje nástroje pro správu malých i velmi rozsáhlých sítí. Pracuje pomocí SNMP protokolu, dokáže prohledávat síť, upozorňovat administrátory na alarmy a výpadky, generovat statistiky a managovat aktivní prvky v síti. Systém je celkově velice škálovatelný a rozsáhlý, umožňuje rychlou implementaci pluginů a optimalizaci pro každou síť.

4.3 Seznam open source software pro monitoring

Počet open-source řešení pro monitoring sítí je relativně rozsáhlý. Pro ukázku uvádím pouze ty nejznámější.

4.3.1 Nagios

Nagios je open-source monitorovací software, zejména používaný k monitorování koncových zařízení v síti a síťových službách. Používá se především k monitoringu dostupnosti zařízení a monitorování služeb typu SMTP, POP3, HTTP, PING. Další z jeho funkcí je definice hierarchie sítě. Podle této hierarchie dokáže definovat dostupná a nedostupná zařízení.

Charakteristika Nagios:

- Zjištění dostupnosti síťových zařízení (echo request = ping)
- Dostupnost síťových služeb (SMTP, FTP, HTTP, SSH. . .)
- Systémové údaje pomocí protokolu SNMP
- Dokáže reagovat na alarmy – email, SMS, zpráva na pager, spustit nějakou akci, restartovat, vypnout

- Podporuje statistiky, záznamy a logy událostí
- Dokáže graficky vykreslit 2D nebo 3D topologii sítě
- Zjišťovaní informací pomocí webového rozhraní

Výhody

- Monitorovaní zařízení bez závislosti na OS
- Monitorování libovolných služeb
- Žádné licenční poplatky
- Dobře otestovaný i ve velmi složitých konfiguracích

Nevýhody

- Vyžaduje serverovou stanici
- Konfigurace probíhá pomocí konfiguračních souborů
- Relativní složitost konfigurace
- Chybí možnost konfigurovat přes webové rozhraní (ve vývoji)

4.3.2 Cacti

Cacti je nástroj pro tvoření grafů síťového provozu. Vychází z nástroje RRD Tool, ale je uživatelsky příjemnější a škálovatelnější. Cacti je naprogramována v PHP, a ke svému provozu potřebuje mysql databázi, RRD tool, Net-SNMP a web server. Je to nástroj, který umožňuje monitorovat a vykreslovat široké množství dat (CPU, paměť, zatížení sítě, obsazení disků, síla signálu). Pro Cacti existuje množství různých pluginů, které rozšiřují její funkci. V základním nastavení Cacti nalezneme pomocné šablony, které nám pomohou sledovat zařízení např. typu Unix/Linux, Windows, Novell, Cisco, tiskárny atd. Tyto šablony si také můžeme vytvářet sami.

Výhody:

- Propracovaná přístupová práva pro uživatele
- Přehledné a graficky upravovatelné výstupy (grafy)
- Využívání vlastních šablon pro specifická zařízení (xml formát)
- Monitoruje dostupnost, při alarmu upozorňuje emailem
- Podpora různých pluginů (NTop, Syslog, MACtrack...)
- Jednoduchá instalace a konfigurace pomocí webového rozhraní

Nevýhody:

- Složitost konfigurace nových šablon
- Vyžaduje serverovou stanici

4.3.3 Dude

Dude je monitorovací nástroj přímo od firmy Mikrotik. Jeho specializací je tedy software RouterOS. Jedná se o vizuálně konfigurovatelný a monitorovací program, pomocí kterého můžeme managovat rozsáhlé sítě, postavené na platformě Mikrotik. Dude nám také umožňuje graficky zobrazovat strukturu sítě, monitorovat a vytvářet statistiky.

Pro získávání dat ze zařízení pracuje Dude jak s protokolem SNMP tak prostřednictvím vzdálené správy RouterOS, implementovaným firmou Mikrotik. Dude neslouží pouze pro statistické záznamy, ale také pro celkový management zařízení. Vyznačuje se hlavně přívětivým uživatelským rozhraním a celkovou jednoduchostí konfigurace. Pro pomoc slouží nástroj „Network Discovery“. Jedná se o nástroj, který automatický vyhledává hosty nebo služby v síti. Podporuje také importy a exporty konfiguračních souborů.

Dude obsahuje dvě části:

Dude server - je to program, který běží na pozadí, nemá žádné uživatelské rozhraní, a může být kontrolován pouze Dude klientem, který může být nainstalován na lokální stanici nebo kdekoliv v síti. Obsahuje také webové rozhraní pro nastavování základních funkcí.

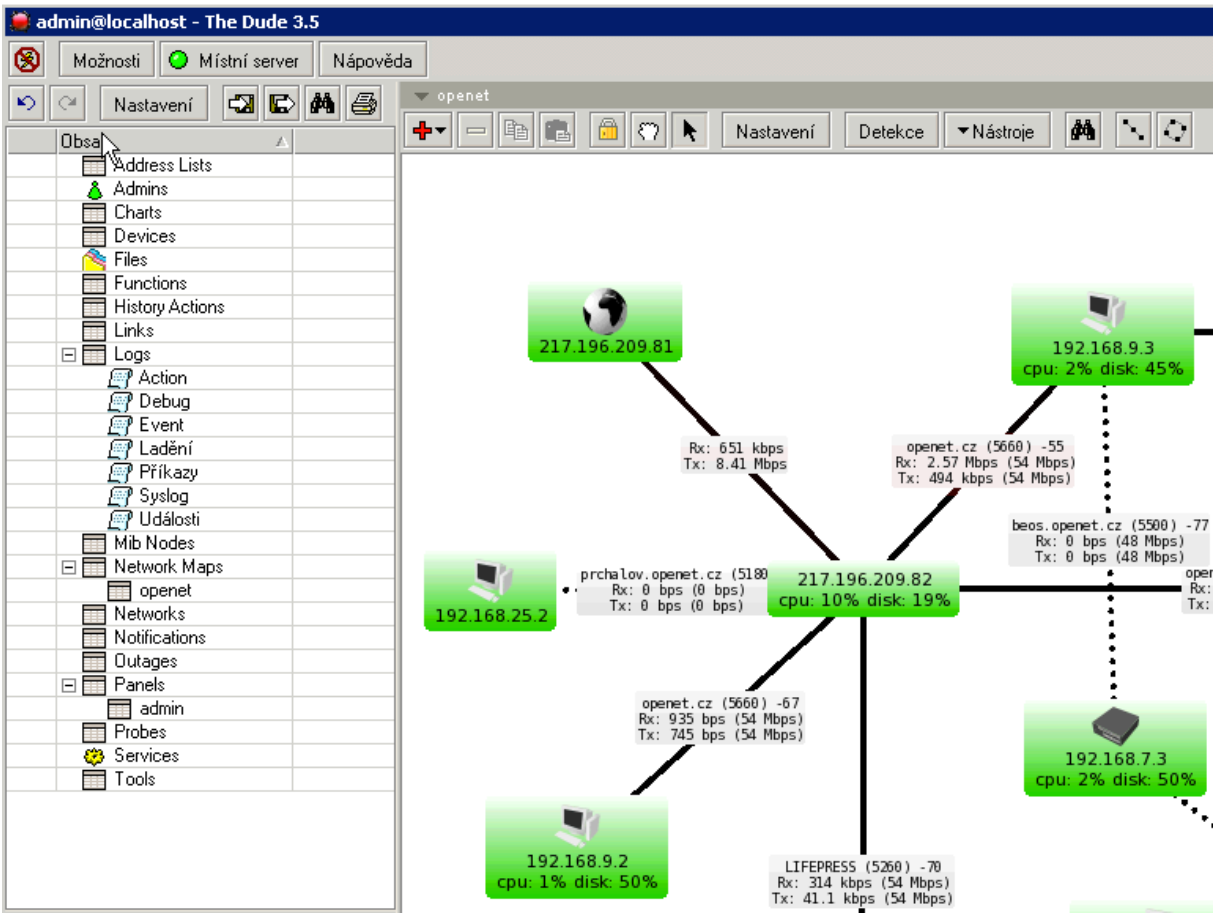
Dude klient – jedná se o klientský program, který se připojuje pouze na Dude server. Obsahuje plnohodnotné grafické uživatelské rozhraní a širokou možnost nastavení. Veškerá nastavení jsou uložena a provedena pouze na serveru, v případě, že by došlo k chybě v přenosu, data zůstanou neporušena. Komunikace mezi Dude klientem a serverem může být buď nešifrovaná nebo šifrovaná. Komunikace při výchozím nastavení běží na portu TCP2210 nešifrovaně a TCP2211 šifrovaně.

Výhody:

- Neomezené možnosti monitorování Mikrotik zařízení
- Nastavení závislosti zařízení
- Příjemné uživatelské rozhraní
- Podpora SNMP protokolu

Nevýhody:

- Vyžaduje serverovou stanici s operačním systémem Windows



Obrázek 4.3 - Ukázka uživatelského rozhraní DUDE

4.3.4 Zabbix

Zabbix je komplexní monitorovací software. Podporuje monitoring pomocí SNMP protokolu, externích skriptů a ICMP testů. Zabbix je schopen monitorovat nejrůznější služby např. mail, webové služby, zatížení rozhraní, dostupnost, atd.

Samotný systém můžeme rozdělit na:

Server pro sběr dat – tvořený pomocí SNMP protokolu. Kontroluje stav konfigurovaných prvků a výsledky ukládá do mysql databáze.

Server pro prezentaci stavu monitorovaných prvků – tvořen pomocí webového serveru a přívětivého uživatelského rozhraní.

Výhody:

- Kvalitní dokumentace
- Jednoduchá instalace z repozitářů

- Kvalitní webové rozhraní

Nevýhody:

- Složitá konfigurace

4.3.5 MRTG

MRTG – Multi Router Traffic Grapher. Jak už název napovídá, jedná se o nástroj zobrazovaní provozu sítě. Je uvolněn pod GNU licencí a jeho autory jsou Toblas Oetiker a Dave Rand. MRTG slouží ke sledování datového provozu na síťovém rozhraní. Tento nástroj nám také generuje grafické přehledy a statistiky pro jednotlivá rozhraní, a rozděluje je do kategorií denní, týdenní, měsíční a roční. SNMP si data komprimuje do vlastního formátu, tím zabraňuje nadměrné velikosti. Grafy jsou zobrazovány buď ve formátu GIF, nebo ve formátu PNG. MRTG ke svému provozu potřebuje SNMP deamona a CRON.

Výhody:

- Jednoduchá instalace z repozitáře
- Přehledné grafy pro jednotlivá rozhranní

Nevýhody:

- Omezené možnosti nastavení

5 Implementace vybraných softwarových nástrojů

Důležitou roli při výběru nástrojů mají tato kritéria:

- Cena
- Podporované systémy
- Webové rozhraní
- Vizuální výstupy
- Jednoduché přidávání zařízení

Pro monitoring bezdrátové sítě opENet jsem na základě potřeb, definovaných v kapitole 3.4, provedl výběr těchto monitorovacích nástrojů.

Nagios – tento softwarový nástroj jsem vybral proto, neboť dokáže rychle reagovat na změny v síti, a také je možné navolit si různé způsoby reakcí na alarmy a možnost definovat různé administrátory pro potřeby upozorňování.

Cacti – jako statistický zobrazovací nástroj jsem použil Cacti. Má široké možnosti použití různých šablon a pluginů, kvalitní řízení přístupových práv a v neposlední řadě možnosti grafických změn a přizpůsobení vzhledů grafů.

Dude – tento nástroj jsem zvolil proto, neboť je přímo od výrobce bezdrátových zařízení, které jsou v síti opENet. Jako hlavní nevýhoda spočívá v menších možnostech využití při monitorování jiných aktivních prvků než od firmy Mikrotik, a také grafické rozhraní pro MS Windows.

Implementaci Nagios a Cacti budeme provádět na linuxovém serveru s operačním systémem Ubuntu 8.10.

root@server:~#uname –a

Linux server 2.6.27-11-server #1 SMP Wed Apr 1 21:53:55 UTC 2009 i686 GNU/Linux

Server bude mít předinstalované následující aplikace: MYSQL, PHP5, Apache2, PEAR, SNMPD.

5.1 Implementace Nagios

Nagios potřebuje ke svému správnému provozu následující aplikace:

- Apache 2
- PHP
- GCC compiler and development libraries
- GD development libraries

Samotná instalace Nagios pro verzi Ubuntu 8.10 je jednoduchá. Instalace bude probíhat z repozitáře. Budeme také instalovat aktuální verzi Nagios, což bude verze 3.

5.1.1 Instalace

Instalaci Nagios3 provádíme z repozitáře:

root@apt-get install nagios3

Můžeme si zkontrolovat konfiguraci:

root@nagios3 –v /etc/nagios3/nagios.cfg

Nagios 3.0.2

Copyright (c) 1999-2008 Ethan Galstad (http://www.nagios.org)

Last Modified: 05-19-2008

License: GPL

Reading configuration data…

Running pre-flight check on configuration data…

Checking services…
    Checked 23 services.
Checking hosts…
    Checked 17 hosts.
Checking host groups…
    Checked 7 host groups.
Checking service groups…
    Checked 0 service groups.
Checking contacts…
    Checked 1 contacts.
Checking contact groups…
    Checked 1 contact groups.
Checking service escalations…
    Checked 0 service escalations.
Checking service dependencies…
    Checked 0 service dependencies.
Checking host escalations…
    Checked 0 host escalations.

Checking host dependencies...

Checked 0 host dependencies.

Checking commands...

Checked 144 commands.

Checking time periods...

Checked 4 time periods.

Checking for circular paths between hosts...

Checking for circular host and service dependencies...

Checking global event handlers...

Checking obsessive compulsive processor commands...

Checking misc settings...

Total Warnings: 0

Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check

Základní nastavení:

Přidání nového uživatele pro přístup na webové rozhraní:

htpassword –c /etc/nagios3/htpasswd.users jmeno_uzivatele

New password: vase_heslo

Re-type new password: vase_heslo

Adding password for jmeno_uzivatele

Nyní se můžeme připojit na webové rozhraní:

http://vase_ip_adresa/nagios3

konkrétně: http://openet.cz/nagios3

Po zadání uživatelského jména a hesla si můžeme prohlédnout základní webové rozhraní.

Konfigurace provádíme pomocí konfiguračních souborů

V hlavním adresáři se nachází:

apache2.conf – nastavení webového serveru
cgi.cfg – hlavní konfigurační soubor pro nastavení práv přístupu
confg.d/ - složka pro konfigurační soubory služeb monitorování

contacts_nagios2.cfg

extinfo_nagios2.cfg

generic-host_nagios2.cfg

generic-service_nagios2.cfg

host-gateway_nagios3.cfg

hostgroups_nagios2.cfg

localhost_nagios2.cfg

services_nagios2.cfg

timeperiods_nagios2.cfg

htpassword.users – konfigurační soubor přístupových jmen a hesel

nagios.cfg – hlavní konfigurační soubor

ndo2db.cfg – deamon konfigurační soubor

ndomod.cfg – deamon konfigurační soubor

objects/ - složka s objekty monitorování

switch.cfg

switchhold.cfg

templates.cfg

resource.cfg – např. definice makra pro rozšířené přístupové práva

stylesheets/ - složka, která obsahuje vizuální kaskádové styly nagios3

5.1.2 Konkrétní nastavení pro síť opENet

Pro korektní nastavení Nagios3 je nutné provést několik nezbytných kroků. Začneme nastavením skupiny administrátorů, kteří budou informováni pomocí emailu na různé druhy alarmů. Potom nastavíme jednotlivé hosty, které chceme monitorovat.

Nastavení souboru: contact_nagios2.cfg

```
##############################################################################
# contact_nagios2.cfg
##############################################################################
##############################################################################
# CONTACTS
##############################################################################
# Nastavení jména kontaktu, emailovou adresu, ap.
define contact{
 contact_name root
 alias Root
 service_notification_period 24x7
 host_notification_period 24x7
```

```
 service_notification_options w,u,c,r
 host_notification_options d,r
 service_notification_commands notify-service-by-email
 host_notification_commands notify-host-by-email
 email nagiosnagiosnagios99@t-email.cz
 }
################################################################################
# CONTACT GROUPS
################################################################################
# Vytvoření skupin kontaktů pro rozsáhlé sítě.
define contactgroup{
 contactgroup_name admins
 alias Nagios Administrators
 members root
 }
```

Nastavení souboru services_nagios2.cfg

```
# check that web services are running
define service {
 hostgroup_name http-servers
 service_description HTTP
 check_command check_http
 use generic-service
 notification_interval 0
}
# check that ssh services are running
define service {
 hostgroup_name ssh-servers
 service_description SSH
 check_command check_ssh
 use generic-service
 notification_interval 0
}
# kontrola dostupnosti pomoci ping
define service {
hostgroup_name ping-servers
service_description PING
```

```
check_command check_ping!100.0,20%!500.0,60%
use generic-service
notification_interval 0 ; set > 0 if you want to be renotified
}
define service{
 use generic-service
 host_name localhost
 service_description SMTP
 is_volatile 0
 check_period 24x7
 max_check_attempts 3
 normal_check_interval 5
 retry_check_interval 1
 #contact_groups conctact
 notification_interval 240
 notification_period 24x7
 notification_options w,u,c,r
 check_command check_smtp
}
```

Nastavení konfiguračního souboru /object/switch.cfg

Pro ukázku zde uvádím pouze část konfiguračního souboru, ale pro bezdrátovou síť opENet jsem musel uvést všechna zařízení v síti, která bych chtěl monitorovat.

```
define hostgroup{
hostgroup_name routers
alias Mikrotik Routers
}
define hostgroup{
hostgroup_name switch
alias SWITCH
}
# qos
define host{
use generic-host
host_name qos
parents gateway
alias qos.openet.cz
```

icon_image rb1000.png

statusmap_image /base/router40.gd2

address 217.196.209.81

hostgroups routers

}

shaping

define host{

use generic-host

parents qos

icon_image rb1000.png

statusmap_image /base/router40.gd2

host_name shaping

alias shaping.openet.cz

address 217.196.209.82

hostgroups routers

}

…

Po nastavení všech konfiguračních souborů zkontrolujeme konfiguraci:

root@nagios3 –v /etc/nagios3/nagios.cfg

Potom provedeme restart služby deamona

root@/etc/init.d/nagios3 restart

Nagios3 je nainstalován a připraven k použití.

5.2 Implementace Cacti

Pro správnou funkčnost Cacti potřebujeme následující balíčky:

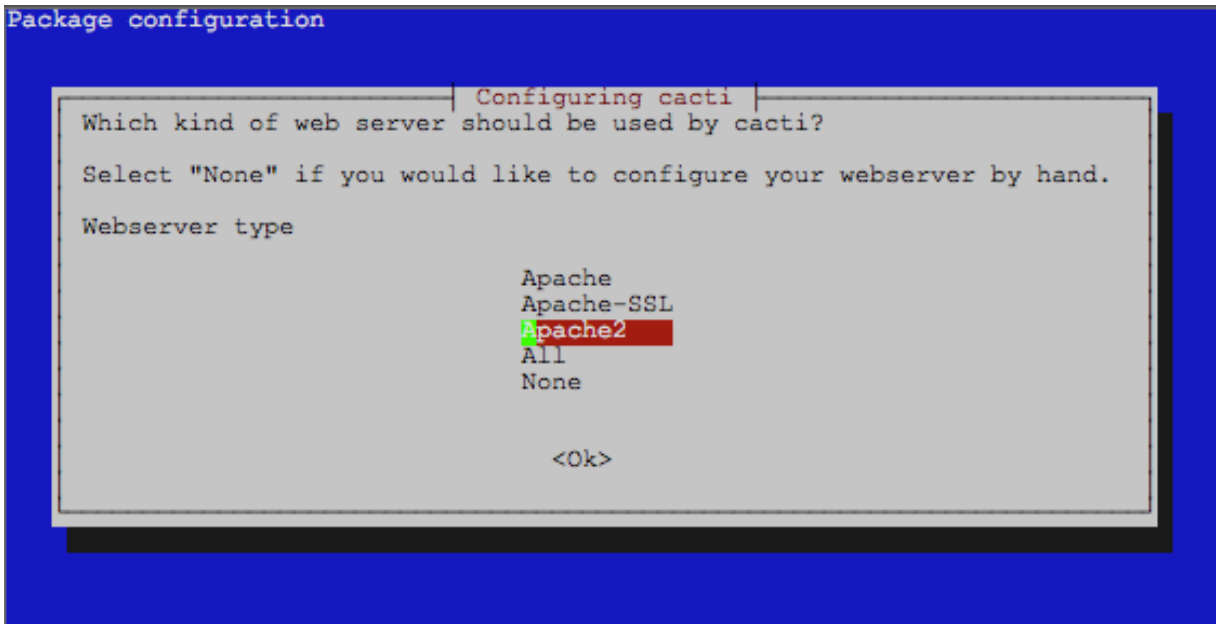
- RRDTool 1.2.x nebo vyšší verzi
- MySQL 4.1.x nebo vyšší verzi
- PHP 4.3.6 nebo vyšší verzi, optimální je PHP 5
- Webový server – Apache, nebo IIS

5.2.1 Instalace

root@apt-get install php5 php5-gd php5-mysql rrdtool

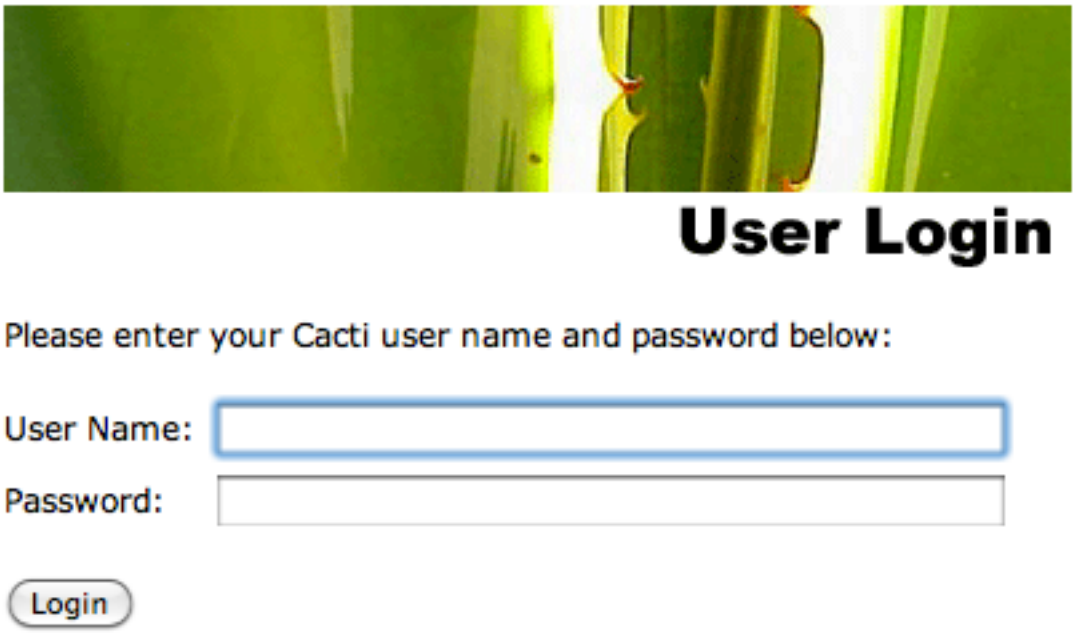
Následující příkaz začne instalovat Cacti a spustí grafického průvodce.

root@apt-get install cacti-cactid



Obrázek 5.1 - Instalační průvodce Cacti

Pro ukázku představím pouze část instalačního procesu. Instalační průvodce nás provede řadou kroků, například nastavení hesla do databáze mysql, nastavení přístupových údajů do webového rozhraní. Po dokončení instalace v příkazovém řádku můžeme přejít na nastavení pomocí webového prohlížeče. Do prohlížeče zadáme http://vase_ip/cacti. Ve webovém prohlížeči se spustí další průvodce, který zkontroluje celkovou konfiguraci a dostupnost všech balíčků na serveru. V závěru se nám zobrazí přihlašovací okno a instalace je dokončena (obrázek č. 5.2).



Obrázek 5.2 - Přihlašovací okno Cacti

5.2.2 Rozvržení konfigurace

Veškerá konfigurace Cacti probíhá přes příjemné uživatelské rozhraní. Abychom mohli monitorovat námi specializované zařízení (Mikrotik), je třeba si z následující stránky stáhnout potřebné šablony (Templates), které jsou určeny přesně pro zařízení Mikrotik. Tyto šablony jsou v XML formátu.

http://forums.cacti.net/about10373.html[1]

Do Cacti jsem importoval následující xml šablony:

- cacti_host_template_mikrotik_queue.xml
- cacti_data_template_mikrotik_queue.xml
- cacti_graph_template_queue_tree_bytes.xml
- cacti_data_query_queue_tree.xml
- ipacmikro.xml

Po importu všech šablon můžeme začít s konfigurací.

Konfiguraci Cacti můžeme rozdělit do několika kroků:

Globální nastavení – v tomto nastavení nastavujeme vlastnosti Cacti, tedy například uživatelské přístupy, verzi protokolu SNMP, cesty k binárním souborům, atd.

[1] Aktualizováno 1.5.2010.

Šablony – v tomto nastavení můžeme importovat/exportovat nebo si prohlížet a upravovat jednotlivé definice šablon (například barvu grafu, v jaké jednotce budou výstupy atd.)

Management grafů – Tato část slouží pro zařízení, které chceme monitorovat. Zde si přidáváme nové zařízení a generujeme grafy. Také zde můžeme vytvářet různé stromové struktury. Pro lepší orientaci můžeme vytvářet skupiny a přidělovat různá práva různým administrátorům.

5.2.3 Konkrétní nastavení pro síť opENet

Postup nastavení Cacti je následující:

Přidání zařízení, které chceme monitorovat

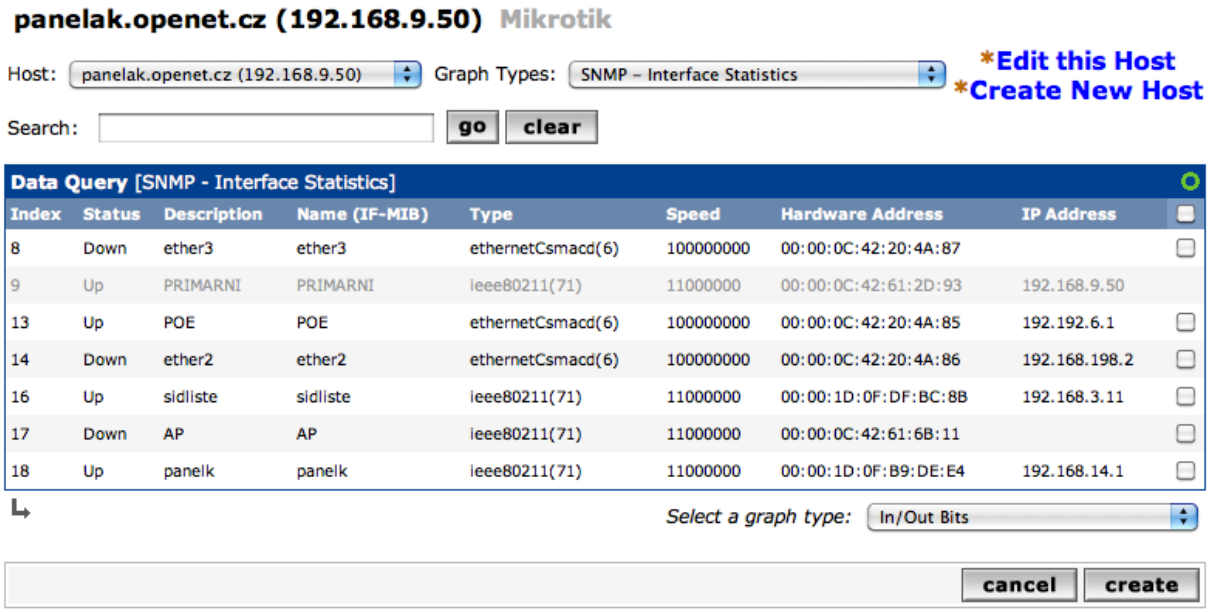
V záložce „devices“ jsem si postupně přidal zařízení, u kterých bych chtěl monitorovat provoz na jednotlivých rozhraních a sílu signálu bezdrátových spojů. Vytvořil jsem si vlastní řetězec komunity a nastavil ho na všech hlavních zařízeních v síti. Potom jsem už jen postupně přidával ip adresy od zařízení, která jsem chtěl monitorovat. Nakonec vypadal seznam zařízení takto: obr. 5.3

<< Previous						Showing Rows 1 to 11 of 11 [1]
Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname
beos.openet.cz	11	2	2	Up	0	192.168.7.1
kadera.openet.cz	13	2	2	Up	0	192.168.2.2
lifepress2.openet.cz	10	2	2	Up	0	192.168.7.2
Localhost	1	5	6	Up	0	127.0.0.1
panelak.openet.cz	5	6	6	Up	0	192.168.9.50
pavelka.openet.cz	12	3	3	Up	0	192.168.9.2
prchalov.openet.cz	14	1	1	Up	0	192.168.25.2
qos.openet.cz	2	123	123	Up	0	217.196.209.81
shaping.openet.cz	3	28	28	Up	0	217.196.209.82
sidliste.openet.cz	8	3	3	Up	0	192.168.2.4
stefan.openet.cz	9	2	2	Up	0	192.168.1.3
<< Previous						Showing Rows 1 to 11 of 11 [1]

Obrázek 5.3 – Seznam záložky „devices“ – Cacti

Vytvoření grafů

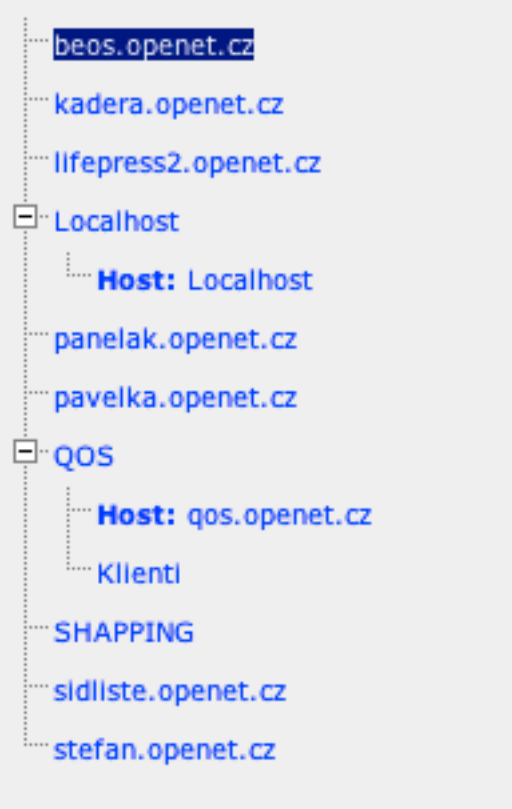
Pro vytvoření grafů slouží záložka „create graphs“ v úvodní obrazovce uživatelského rozhraní. Po rozkliknutí možnosti se nám zobrazí seznam všech zařízení přidaných v Cacti a také dostupné grafy, které můžeme pro jednotlivá zařízení vytvořit. Potom už jen v našem případě označíme rozhraní, které chceme monitorovat (obrázek č. 5.4) a klikneme na tlačítko „create“. Tuto možnost jsem postupně vytvořil pro všechny ostatní zařízení v síti.



Obrázek 5.4 – Vytvoření konkrétního grafu – Cacti

Vytvoření přehledné struktury

Cacti umožňuje vytvářet přehledné a stromové struktury vašich grafů. Pro přehlednost jsem vytvořil samostatnou skupinu pro každé zařízení, a do této skupiny jsem vložil grafy síly signálu a zatížení požadovaného rozhraní. Pro monitoring všech klientů jsem vytvořil skupinu QOS, a do ní přidal grafy datového přenosu každého klienta sítě opENet.



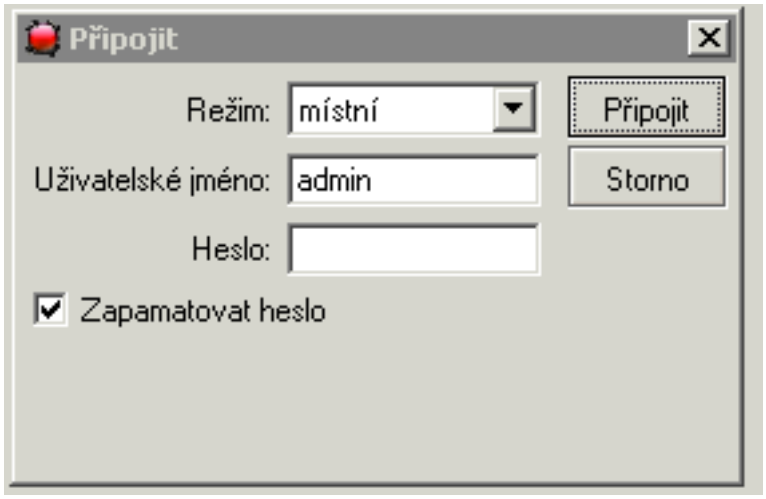
Obrázek 5.5 – Přehledná struktura grafů – Cacti

Tímto nastavením jsme získali přehled využití připojení internetu a také jsme zjistili sílu signálu pro páteřní spoje.

5.3 Implementace Dude

5.3.1 Instalace

Instalace Dude není vůbec složitá. Na webových stránkách: http://www.mikrotik.com/thedude.php[2] si stáhneme instalátor pro Windows 2003 server. Tento software můžeme instalovat i na Linux (přes Wine), ale pro naše účely se nám hodí více Windows, protože na Linuxovém stroji nemáme žádné vhodné grafické uživatelské rozhraní. Po ukončení instalátoru spustíme DUDE. Spustí se nám DUDE client, a my se můžeme pomocí defaultního jména a prázdného hesla přihlásit na server.



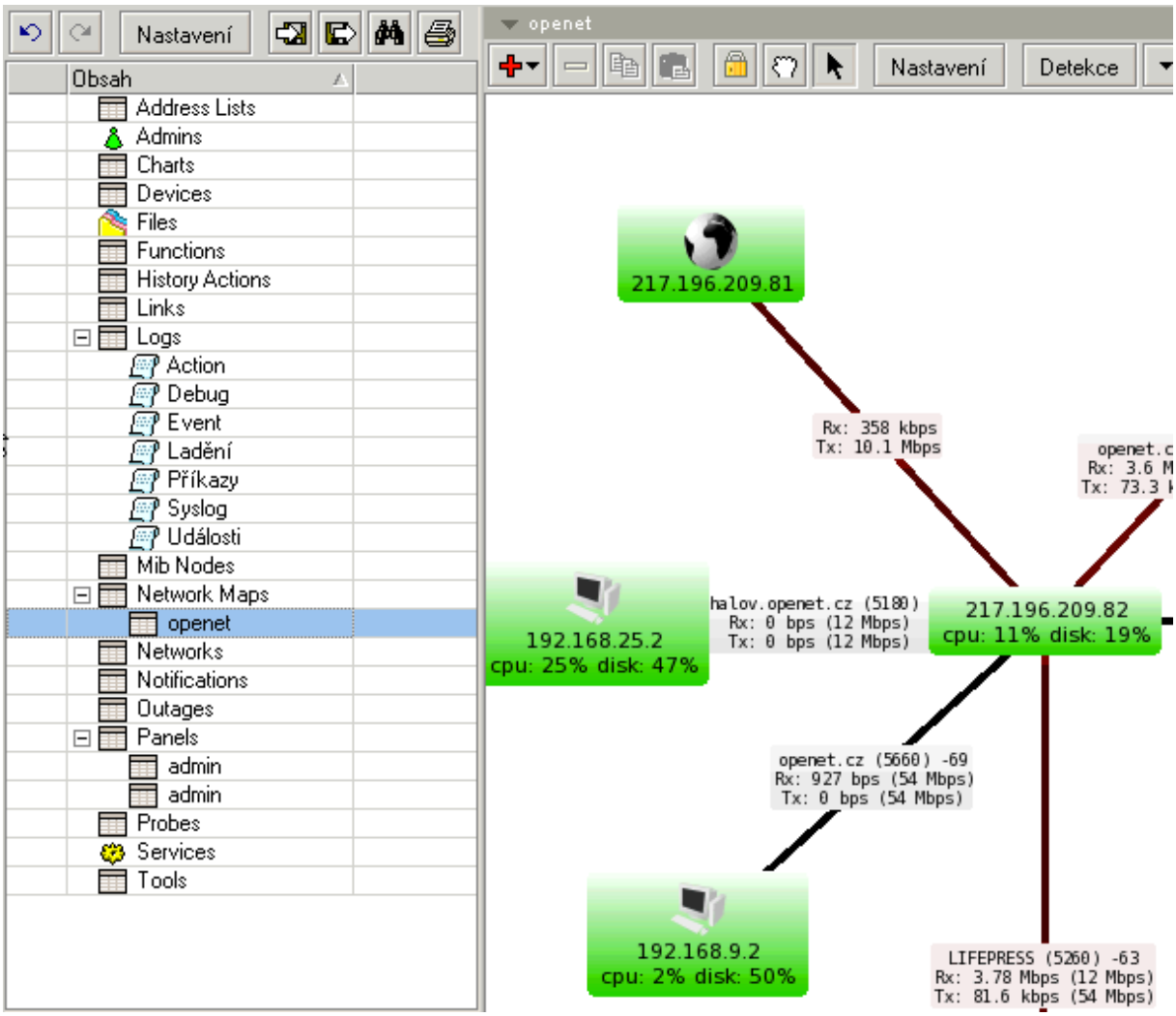
Obrázek 5.6 - Přihlašovací okénko DUDE klienta

5.3.2 Konkrétní nastavení pro síť opENet

Konfigurace Dude je velice přívětivá a intuitivní, a grafické rozhraní nám dokonce nabízí přepnout do českého jazyka.

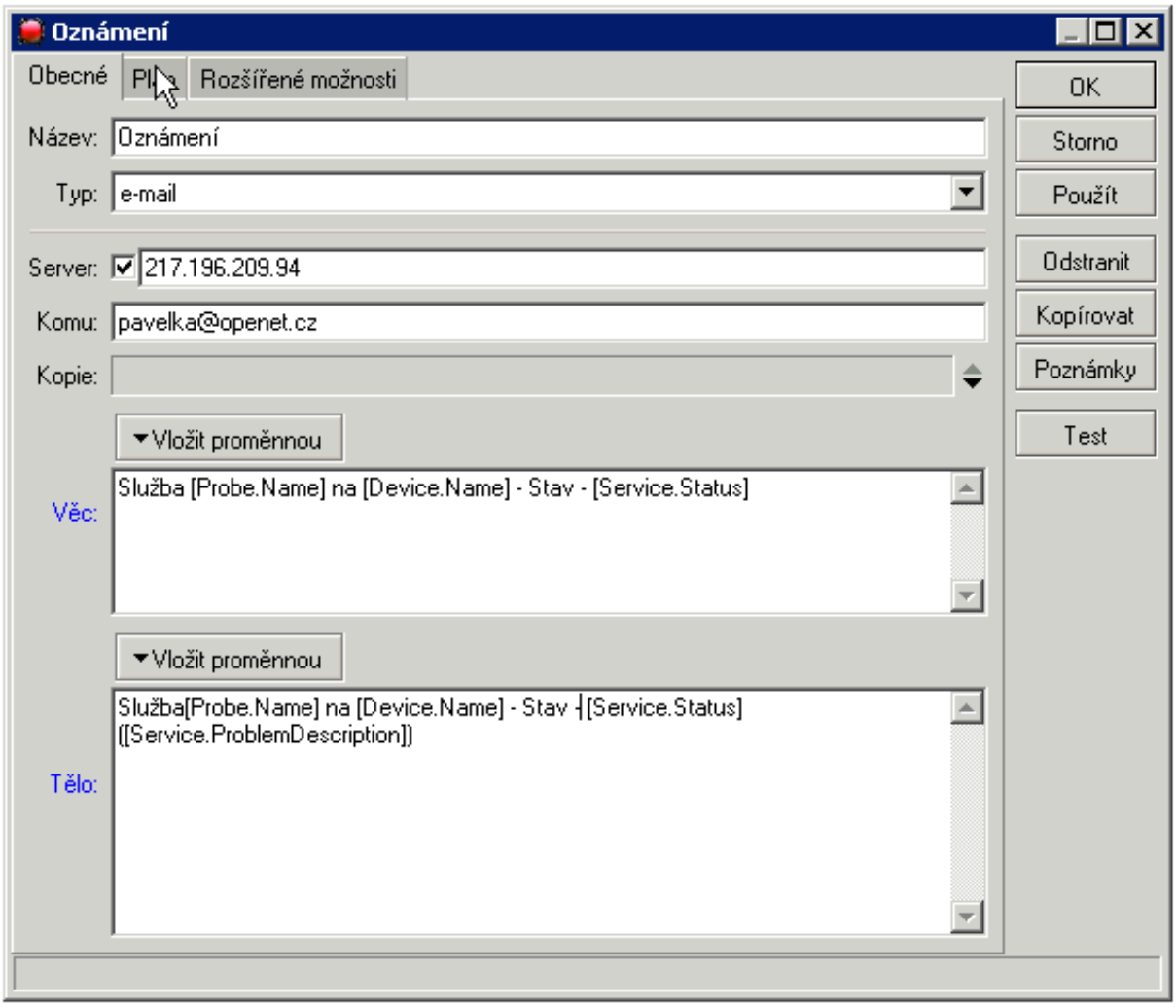
Konfiguraci jsem začal tak, že jsem si nejdříve vytvořil a pojmenoval vlastní mapu sítě opENet (záložka *network maps*), a postupně přidával zařízení, u kterých jsem po řadě doplnil potřebné údaje pro SNMP (řetězec komunity) a také pro RouterOS (login, heslo).

[2] Aktualizováno 1.5.2010



Obrázek 5.7 - Zařízení přidané do mapy sítě a jejich zobrazení

Další nastavení se týkalo alarmů a způsobů upozornění na případný výpadek služby nebo zařízení. Do záložky *Notification* jsem přidal nová upozornění, a vyplnil patřičné údaje, tedy SMTP server, email administrátora a tělo zprávy.



Obrázek 5.8 - Nastavení způsobu upozornění na email

6 Ověření funkce v ostrém provozu

Po měsíci testování výše uvedené konfigurace systém pracuje spolehlivě. V praxi jsou asi nejdůležitějším výstupem automaticky zasílaná chybová upozornění ze systémů Nagios. Tato upozornění informují o dostupnosti zařízení, a tedy o funkčnosti internetu.

Dalším pozitivním přínosem byly grafické výstupy zatížení jednotlivých spojů z Cacti. Podle těchto údajů jsem mohl přepojit některé uživatele, a rozložit tak provoz přes vhodnější bezdrátová zařízení. Tyto údaje mi pomohly zlepšit celkovou odezvu sítě mezi jednotlivými bezdrátovými zařízeními.

Nástroj Dude jsem použil při analýze například routovacích tabulek, ospf protokolu a analýzou protékaných dat v real-time. Tento nástroj je obecně vhodnější pro management a konfiguraci Mikrotik zařízení.

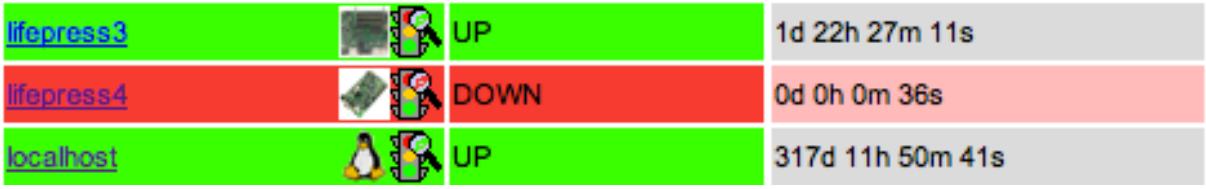
Pro ukázku zobrazuji množství výstupů, které jednotlivé programy nabízejí.

6.1 Výstupy Nagios

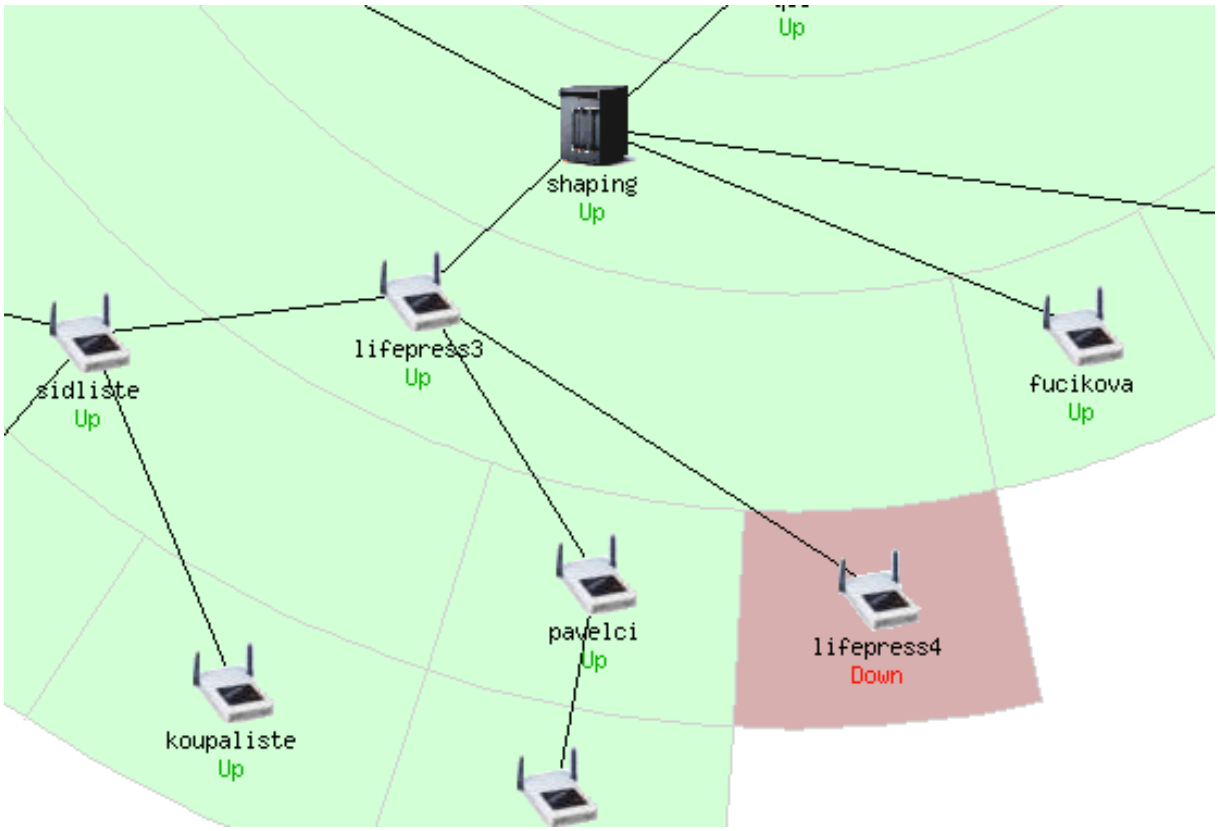
Po otestování konfigurace Nagios3 jsem vytvořil následující mapu bezdrátové sítě opENet a vytvořil níže uvedené závislosti služeb (obrázek č. 6.2).

Při výpadku nebo upozornění některé z monitorovaných služeb, je administrátorovi zaslána zpráva na emailovou adresu, která je potom pomocí GSM T-MOBILE služby přeposlána na mobilní telefon. Po měsíci testovaní se služba chová dobře, a dá se říci, že vše funguje velice spolehlivě. Tato zpráva podle způsobu upozornění obsahuje například:

** Nagios **
Typ upozorneni: PROBLEM
Sluzba: PING
Host: lifepress4.openet.cz
Adresa: 192.168.2.4
State: PROBLEM
Date/Time: Sun Apr 18 16:19:42 CEST 2010



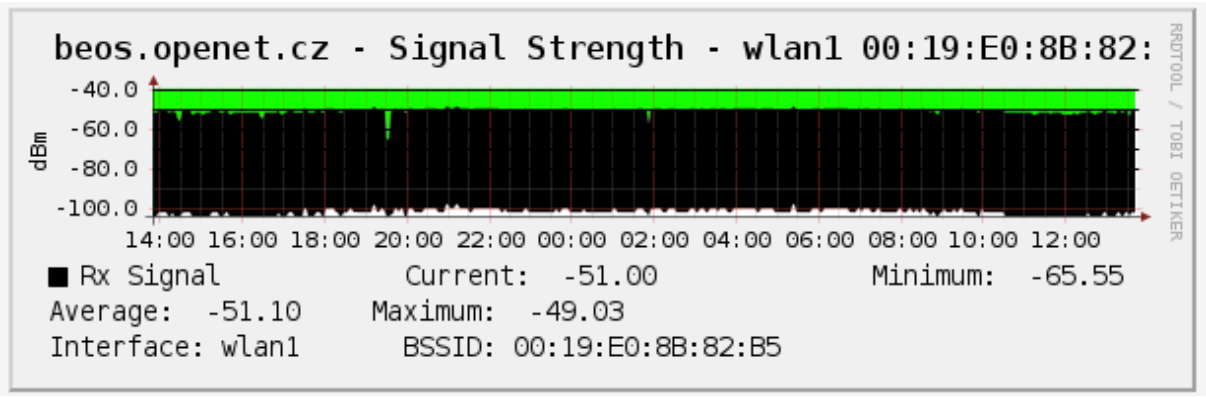
Obrázek 6.1 - Zobrazení výpadku hosta lifepress4



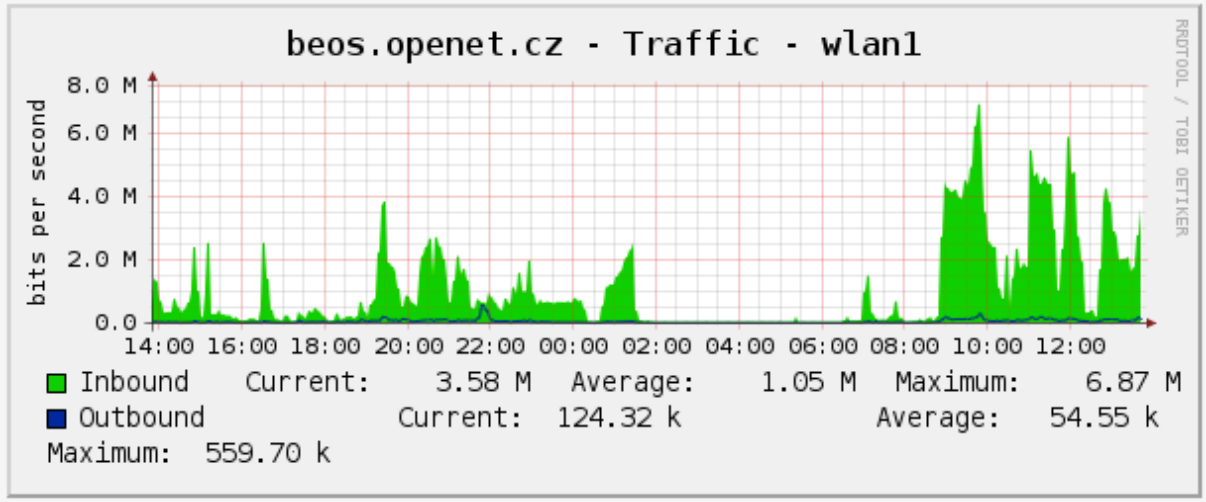
Obrázek 6.2 - Zobrazení výpadku hosta lifepress4

6.2 Výstupy Cacti

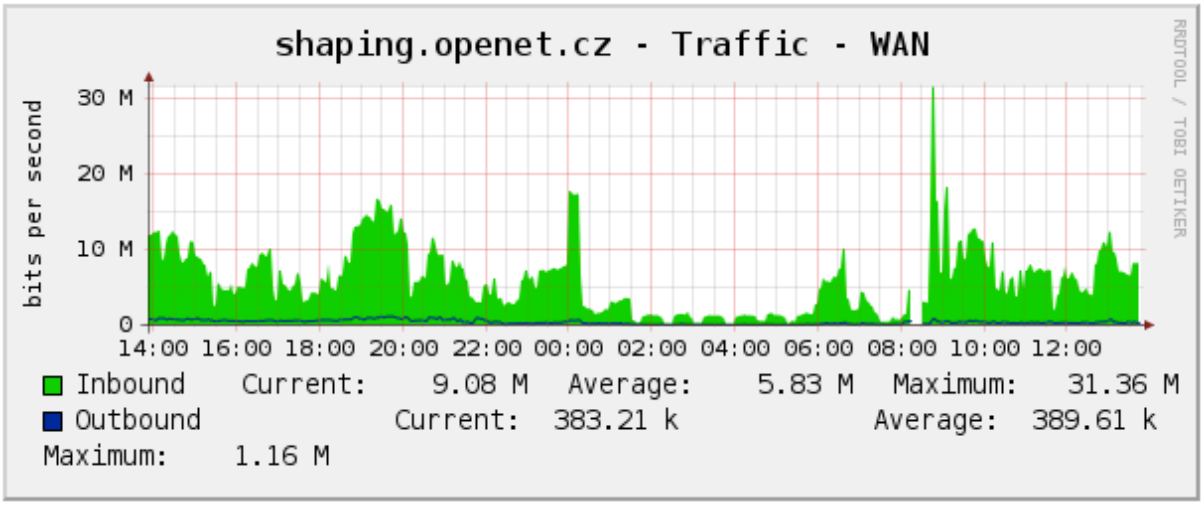
Cacti umožňuje vytvářet přehledné statistiky a stromové struktury grafů zařízení umístěných v síti. Pro ukázku zobrazím pouze část grafů a část zařízení, která jsou monitorována.



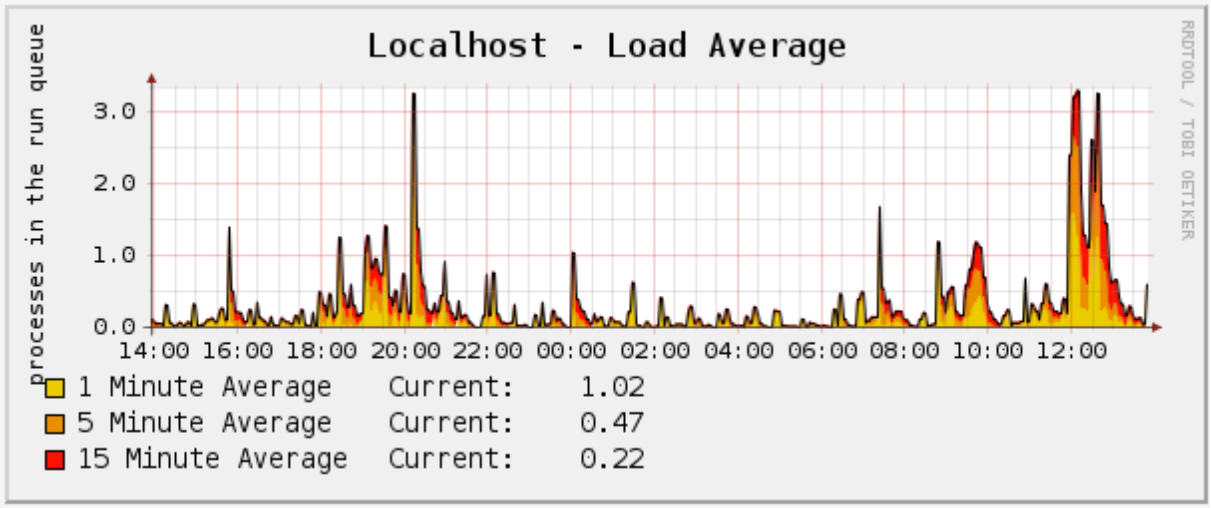
Obrázek 6.3 – Síla signálu pro hosta beos.openet.cz (denní – 5 minutový průměr)



Obrázek 6.4 – Zatížení bezdrátového rozhraní u hosta beos.openet.cz (denní – 5 minutový průměr)



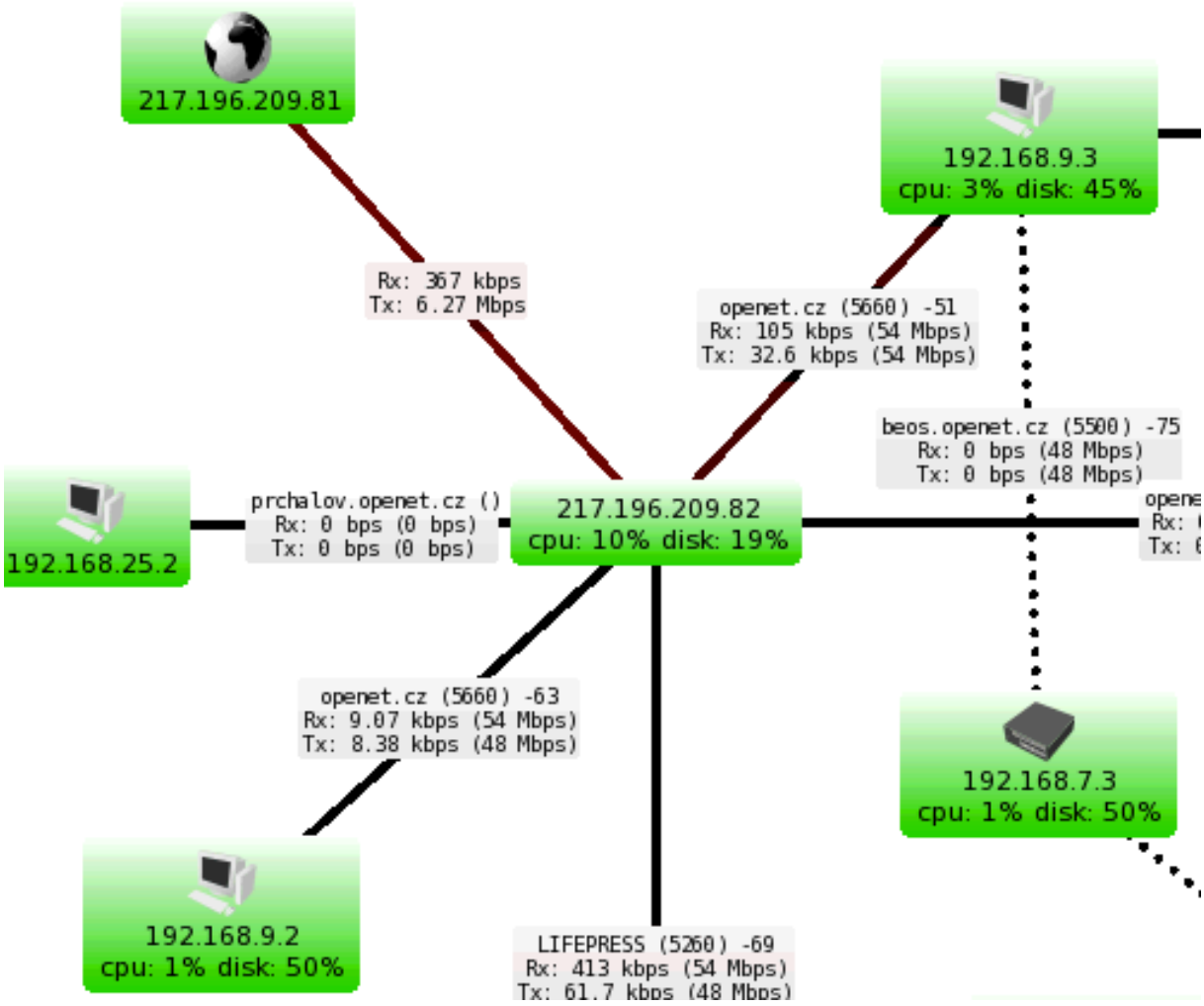
Obrázek 6.5 – Statistiky hlavní konektivity



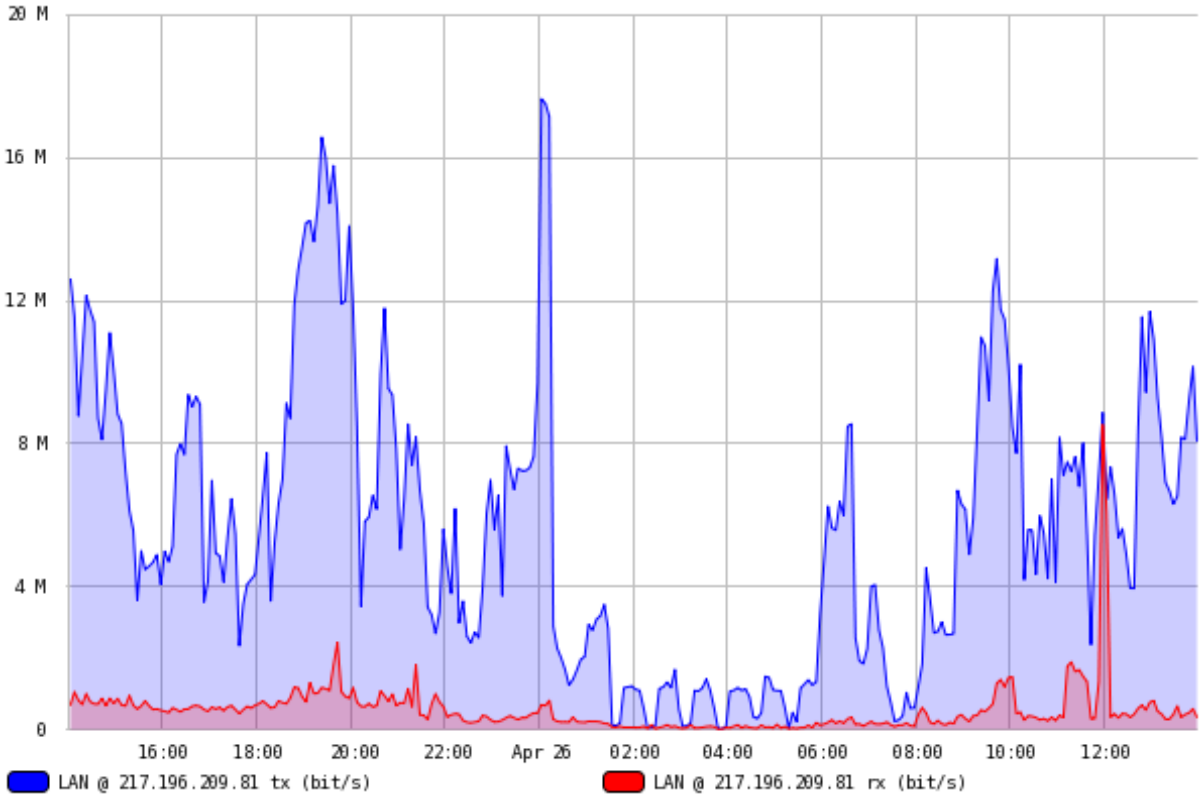
Obrázek 6.6 – Zatížení procesoru webového serveru (denní – 5 minutový průměr)

6.3 Výstupy Dude

Program Dude je komplexní nástroj hlavně pro management zařízení Mikrotik v síti. Pomocí tohoto nástroje můžeme pohotově měnit konfiguraci jednotlivých zařízení v síti a okamžitě zjistit dopad našeho nastavení na naši síť.



Obrázek 6.7 - Mapa sítě v programu DUDE



Obrázek 6.8 – Týdenní graf zatížení WAN rozhraní

7 Závěr

Obecným úkolem monitorování sítí je předávání konkrétních informací o stavu sítě administrátorovi nebo uživatelům. Mezi hlavní požadavky bývá celková dostupnost sítě, vytížení jednotlivých rozhraní a také potenciální bezpečnostní problémy.

Po výběru nejvhodnějších monitorovacích nástrojů jsem v této bakalářské práci implementoval a otestoval Open Source monitorovací nástroje Cacti, Nagios a Dude na komerční bezdrátové síti opENet. Nástroj Nagios jsem primárně určil k monitoringu dostupnosti zařízení a služeb v síti. V případě problému nebo překroční určitých hodnot bude automaticky informován administrátor sítě, který na základě těchto informací může rychleji a lépe analyzovat problém. Nástroj Cacti jsem použil pro vizuální zobrazení statistik jednotlivých klientů, dále pak síly signálu na bezdrátových zařízeních a také zatížení procesoru a vytížení hlavní konektivity. Tyto statistiky například slouží k analýze zařízení, které se musí vyměnit z důvodu zatížení nebo také přesměrování provozu přes jiný bezdrátový bod, či rovněž rapidní snížení síly signálu, což vede ke snížení celkové propustnosti bezdrátového spoje apod. Nástroj Dude jsem použil jako hlavní managovací nástroj, a pomocí tohoto nástroje lze řešit různé problémy spojené s provozem sítě.

Věřím, že výsledky této bakalářské práce výrazně usnadní správu a dohled nad sítí opENet, usnadní analýzu potenciálních problémů a umožní správcům mít přehled nad všemi zařízeními a jednoduše měnit nastavení.

Informace v této bakalářské práci také mohou být nápomocny při budování monitoringu jakékoli počítačové sítě.

Potenciální zdokonalení monitoringu bezdrátové sítě opENet bych rád rozšířil pomocí implementace dalších pluginů pro Cacti, která následně stává mocným nástrojem při dohledu jakékoliv sítě.

8 Literatura

Elektronické zdroje:

Vznik a principy SNMP. *Svět sítí : Správa počítačových sítí* [online]. 11. června 2000. [cit. 2010-04-05]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=29>.

About Cacti. *Cacti : the complete rrdtool-based graphing solution* [online]. 2004 [cit. 2010-45-05]. Dostupný z WWW: <http://www.cacti.net/>.

AdminXP.cz. *Networking : SNMP Jednuduchý management sítě* [online]. 2010 [cit. 2010-04-05]. Dostupný z WWW: <http://www.adminxp.cz/networking/index.php?aid=21>.

Formát SNMP zpráv. *Svět sítí : Správa počítačových sítí* [online]. 11. června 2000. [cit. 2010-04-05]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=32>.

Mikrotik vizualizace datových toků. *Mikrotic* [online]. 2010, 1, [cit. 2010-04-05]. Dostupný z WWW: <http://download.asm.cz/inshop/prod/xtendlan/Mikrotik/EM-Mikrotik-Vizualizace_datovych_toku.pdf>.

Routers and Wireless : *The Dude* [online]. 2010 [cit. 2010-04-03]. Dostupné z WWW: <http://www.mikrotic.com/thedude.php>.

Nagios : *Documentation* [online]. 2010 [cit. 2010-04-03]. Dostupné z WWW: <http://support.nagios.com/knowledgebase>.

Monografie:

MATŮŠŮ, Jindřich. *Diplomová práce : Monitorování stavu rozsáhlých sítí*. Ostrava, 2008.

SLÉŽKA, Jiří. *Diplomová práce: Realizace monitoringu síťové infrastruktury Slezské univerzity* v Opavě. Opava, 2007.

ZANDL, Patrick. *Bezdrátové sítě WiFi*. Praha : Computer Press, 2003. 204 s. ISBN 80-722-6632.